Commonwealth of Virginia Data Trust User Agreement

The Commonwealth of Virginia Data Trust User Agreement (the "Agreement") is entered into on _____ __, 20___ ("Effective Date") by and between the undersigned (hereinafter referred to as "Data Trust User"), and the Chief Data Officer for the Commonwealth of Virginia as the Trustee of the Commonwealth of Virginia's Data Trust ("Trustee"). Data Trust User and Trustee may each individually be referred to herein as a "Party" and collectively as the "Parties."

I. PURPOSE

A. The purpose of the Virginia Data Trust User Agreement is to establish the standards and protocols under which the Data Trust User shall receive, use or transmit data obtained from the Commonwealth of Virginia's Data Trust ("Data Trust"). All data provided through the Virginia Data Trust to the Data Trust User are subject to this Agreement. All information derived from that data, and the data resulting from a merge, match, or other manipulation of the data with other data, are subject to this Agreement and shall be considered Restricted-Use Data.

II. AGREEMENT

A. The following Exhibits shall be made a part of this Agreement for all purposes only upon approval by the Trustee:

1. A description of the proposed project (Exhibit A);
2. A data protection security plan for the Restricted-Use data (Exhibit B);
3. Data Trust Individual User Non-Disclosure Agreement ("Non-Disclosure Agreement") and Non-Disclosure Agreement Registry (Exhibit C);
4. Specific agency-supplied terms identifying additional restrictions or constraints (Exhibit D);
5. List of requested data elements (Exhibit E); and
6. Ethical Principles (Exhibit F).

B. The Trustee has the unqualified right to terminate this Agreement at any time for any reason. Data Trust User also agrees that the Trustee has the unqualified right to revoke the Data Trust User's access or a Data Trust Individual User's access to the Data Trust at any time.

III. DEFINITIONS

A. **In this Agreement**:

1. **"Data Trust Member"** shall mean an organization that has been approved to participate in the Data Trust and be a party to the Data Trust Agreement. Data Trust Members may include private companies, non-profit organizations, philanthropic and governmental entities, and community and/or advocacy groups as determined and approved by the Trustee.

2. **"Data Trust Individual User"** shall mean individuals listed in Exhibit A by the Data Trust User, who have executed a Non-Disclosure Agreement (Exhibit C), and are provided access to Restricted-Use Data.

3. **"Merging Restricted-Use Data Records with Public-Use Data Records"** shall mean a file containing both Restricted-Use Data and Public-Use Data merged into one file.

4. **"Public-Use Data"** shall mean data that contains no personally identifiable or sensitive information which requires no specific procedures to protect confidentiality and is otherwise classified as Tier 0 Data.

5. **"Restricted-Use Data"** shall mean Tier 1, Tier 2, Tier 3, or Tier 4 data that requires specific procedures to protect confidentiality.

6. **"Tier 0 Data"** shall mean data or information this is neither sensitive nor proprietary intended for public access provided on an ongoing basis or as a one-time transfer to Trustee by Data Trust Member for use by Data Trust under this Agreement as detailed in Exhibit B attached hereto or subsequently contributed by Data Trust Member detailed in the Data Trust electronic metadata registry.

7. **"Tier 1 Data"** shall mean data that is not protected from public disclosure or subject to withholding under any law, regulation, or contract. Nevertheless, publication of the dataset on the public Internet and exposure to search engines would: have the potential to jeopardize the safety, privacy, or security of a person who may be identified through use of the data; requires subjective redaction to classify the data as Tier 0 data; impose an undue financial or administrative burden on the Data Trust Member; or expose the Trustee or Data Trust Member to litigation or liability.

8. **"Tier 2 Data"** shall mean sensitive or proprietary information intended for access or release only on a 'need-to-know' basis, including personal information not otherwise classified as Tier 0 or 1, and data protected or restricted by contract, grant, or other agreement terms and conditions provided on an ongoing basis or as a one-time transfer to Trustee by Data Trust Member for use by Data Trust under this Agreement as detailed in Exhibit B attached hereto or subsequently contributed by Data Trust Member and detailed in the Data Trust electronic metadata registry.

9. **"Tier 3 Data"** shall mean sensitive or proprietary information and data elements with a statutory requirement under Data Trust Member's relevant state and federal laws for notification to affected parties in case of a confidentiality breach (e.g. Social Security Number, driver's license number, financial account numbers, personal medical information, etc.) provided on an ongoing basis or as a one-time transfer to Trustee by Data Trust Member for use by Data Trust under this Agreement as detailed in Exhibit B attached hereto or subsequently contributed by Data Trust Member and detailed in the Data Trust electronic metadata registry. Examples of Tier 3 Data may include, but not limited to: Attorney-Client Privileged; Criminal Justice Information; Critical Infrastructure Information; Family Educational Rights and Privacy Act (FERPA); Federal or State Tax Information; or Protected Health Information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA).

10. **"Tier 4 Data"** shall mean sensitive or proprietary data where the unauthorized disclosure could potentially cause major damage or injury, including death, to entities or individuals identified in the information, or otherwise significantly impair the ability of the Data Trust Member to perform its statutory functions. Tier 4 Data includes any dataset designated by a federal agency at the level "Confidential" or higher under the federal government's system for marking classified information. No Tier 4 data shall be knowingly incorporated into the Data Trust.

IV. DATA TRUST USER RESPONSIBILITIES

A. Data Trust User shall comply with the terms of this Agreement and any and all security requirements issued by the Commonwealth of Virginia or the Trustee.

B. Data Trust User agrees that the data provided by the Trustee or through the Data Trust shall remain the property of the Data Trust Member. Data Trust User agrees to destroy any and all Restricted-Use Data upon the request of the Trustee. Data Trust User shall notify the Trustee when the Restricted-Use Data has been destroyed.

C. The Data Trust User shall only use the Restricted-Use Data in a manner consistent with the stated purpose for which the data was supplied pursuant to the proposed project described in Exhibit A. Data Trust User also acknowledges that Tier 4 Data is not meant for access, receipt, or use by Data Trust User. Data Trust User agrees to immediately

notify Trustee if any Tier 4 Data is received and to destroy said Tier 4 Data upon Trustees instructions.

D. Only individuals listed in Exhibit A by the Data Trust User and who have executed a Data Trust Individual User Non-Disclosure Agreement, attached hereto as Exhibit C and hereinafter referred to as "Non-Disclosure Agreement", shall have access to the Restricted-Use Data. The Data Trust User shall provide a copy of this Agreement, together with the attached security plan (Exhibit B) to each Data Trust Individual User. The Data Trust User shall ensure that each individual who executes a Non-Disclosure Agreement reads and understands the materials provided to her or him before executing the Non-Disclosure Agreement.

E. The Data Trust User shall promptly, after the execution of each Non-Disclosure Agreement, send the original or a digital copy of the Non-Disclosure Agreement to the Trustee and keep a copy as part of its security procedures.

F. The Data Trust User shall immediately notify the Trustee when a Data Trust Individual User is no longer authorized to have access to Restricted-Use Data.

G. The Data Trust User shall not publish or disclose Restricted-Use Data to any organization or to any persons without the express written approval of the Trustee.

H. The Data Trust User shall notify the Trustee immediately upon receipt of any legal, or other demand for disclosure of Restricted-Use Data.

I. The Data Trust User shall notify the Trustee immediately upon discovering any breach or suspected breach of this Agreement, including breach of security or any disclosure of Restricted-Use Data to unauthorized parties, agencies or individuals and provide the names and contact information of any individuals involved.

J. The Data Trust User shall maintain personnel policies that subject employees to disciplinary action, including termination for actions that violate the employee's Non-Disclosure Agreement, or cause a violation of this Data Trust User Agreement. The Data Trust User agrees that any Data Trust Individual User whose actions or behaviors that violate the Non-Disclosure Agreement or cause noncompliance with this Data Trust User Agreement shall be removed from the project and Exhibit A and shall not have access to any data, information, materials, items and etc. from the Data Trust.

K. The Data Trust User shall have a valid and enforceable agreement with each of its individual users that require each individual user to, at a minimum: (i) comply with all applicable law; (ii) reasonably cooperate with the Data Trust User on issues related to this Agreement; (iii) transact data only for a permitted purpose; (iv) use data received from the Data Trust in accordance with the terms and conditions of this Agreement; and (v) refrain from disclosing to any other person any passwords or other security measures issued to the individual user by the Data Trust User. Notwithstanding the foregoing,

compliance with this Section may be satisfied through written policies and procedures that address items (i) through (v) of this Section so long as the Data Trust User can document that there is a written requirement that the individual user must comply with the policies and procedures.

L. Data Trust User shall immediately notify the Trustee if any individual identified in Exhibit A, or any of its employees or agents, fails to comply with the provisions of this Agreement or fails to maintain or use Restricted-Use Data in accordance with this Agreement.

V. DATA TRUST USER SECURITY REQUIREMENTS

A. The Data Trust User shall keep the Restricted-Use Data supplied by Trustee in a single, secure location and shall make no copy or extract of the Restricted-Use Data to anyone except those specifically authorized in Exhibit C.

B. The Data Trust User shall maintain Restricted-Use Data in a space limited to access by authorized personnel identified in this Agreement.

C. The Data Trust User shall transport or transmit Restricted-Use Data in a secure manner by authorized personnel only.

D. The Data Trust User shall ensure that access to Restricted-Use Data maintained in Data Trust User's computer systems and networks is controlled in accordance with the security policies and controls identified in Exhibit B and appropriate administrative, physical, and technical safeguards that protect the confidentiality, integrity and availability of data.

E. The Data Trust User shall maintain all hard copy, personal computers with Restricted-Use Data on hard disks, or other physical products containing sensitive, de-identified, record-level information derived from Restricted-Use Data in locked cabinets, file drawers, or other secure locations when not in use.

F. The Data Trust User shall ensure that all hard copy, tabulations, reports, and products are reviewed and edited for any possible disclosures of Restricted-Use Data prior to Publication pursuant to Section XII and/or disclosure of any data from the Data Trust.

G. Each Data Trust User shall ensure that it employs security controls that meet applicable industry, Commonwealth of Virginia and Federal standards so that the data being transacted and any method of transacting such data will not introduce any viruses, worms, unauthorized cookies, trojans, malicious software, "malware," or other program, routine, subroutine, or data designed to disrupt the proper operation of a system or any part thereof or any hardware or software used by a user in connection therewith, or which, upon the occurrence of a certain event, the passage of time, or the taking of or failure to take any action, will cause a system or any part thereof or any hardware, software or data used by a user in connection therewith, to be improperly accessed, destroyed, damaged,

or otherwise made inoperable. In the absence of applicable industry standards, each Data Trust User shall use all commercially reasonable efforts to comply with the requirements of this Section.

H. Each Data Trust User shall be responsible for procuring and ensuring that its individual users have access to all equipment and software necessary for it to access and use the Data Trust. The Data Trust User shall ensure that all computers and electronic devices owned or leased by the Data Trust User and its individual users to be used to access and use the Data Trust are properly configured, including, but not limited to, the base workstation operating system, web browser, and Internet connectivity.

VI. TRUSTEE RESPONSIBILITIES

A. Trustee is responsible for providing the necessary technical and organizational infrastructure to support the creation, use, and maintenance of the Data Trust and ensure all Data Trust Users are in compliance with the terms and conditions of their agreement(s).

B. Trustee will ensure that no Tier 1, Tier 2, or Tier 3 data in its raw form will be included in any published data. During the implementation of Projects and Allowable Uses, Trustee, Data Trust Members, and approved Data Trust Users may develop aggregate data that qualifies for Tier 0 classification as defined by the privacy and anonymization criteria adopted by the Data Governance Council. Such aggregate data may be published in accordance with all other Tier 0 data, as determined by the Data Governance Council. However, prior to any such release, Data Trust Members that own data used in the creation of aggregate data shall be able to review the aggregate data to verify that no Tier 1, Tier 2, Tier 3 or Tier 4 data is revealed.

C. The Trustee will register and make available the names of all approved Data Trust Users, Descriptions of Proposed Projects (Exhibit A), and the names of the Data Trust Individual Users as directed by the Data Governance Council.

D. ANY DATA, DERIVED DATA, AGGREGATE DATA, TRUST-OWNED DATA, AND RESEARCH OUTPUTS CREATED UNDER THIS AGREEMENT ARE PROVIDED "AS IS." THE TRUSTEE AND THE DATA TRUST MEMBERS MAKE NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE WORK OR PRODUCTS OF WORK CREATED UNDER THIS AGREEMENT, INCLUDING ANY EXPRESS OR IMPLIED WARRANTIES OF NON-INFRINGEMENT, OWNERSHIP, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE OF THE DATA GENERATION, RESEARCH OR ANY INVENTION OR PRODUCT.

VII. APPROVED USES

A. Each Data Trust User shall have Data Trust Individual User access policies. Each Data Trust User acknowledges that the access policies will differ among them as a result of differing applicable law and business practices. Each Data Trust User shall be responsible for determining whether and how to access and use the Data Trust based on the application of its access policies to the information from the Data Trust. The Data Trust User agrees that each of its Data Trust Individual Users shall comply with applicable law and this Agreement. It is strictly the Data Trust User's responsibility to add or remove individual users in Exhibit A, ensure such users have signed their respective Non-Disclosure Agreement, and provide the signed documents to the Trustee.

B. Academic research is an approved use of the Trust-managed Data Resources. The Trustee shall make available a secure Data Trust Access Hub ("Access Hub") for access by approved Data Trust Users and put in place a process for certifying access to Trust-managed Data Resources through the Access Hub.

C. Data Trust Users may submit a proposal for the use of Trust-managed Data Resources that requires access to one or more Data Trust Member's Tier 1, Tier 2, or Tier 3 data. This proposal must be submitted in writing to the Trustee. Access to Tier 1, Tier 2 or Tier 3 data will only be provided if the proposal is approved by the Trustee and by the Data Trust Member(s) whose data will be accessed. Data Trust Members retain the right to opt out of the use of their data in any particular project at any time.

D. If applicable, Data Trust Users shall be required to complete relevant Institutional Review Board approval prior to approval for access and use of Trust-managed Data Resources.

E. Merging Restricted-Use Data Records with Public-Use Data Records shall be considered Restricted-Use Data. Merely deleting identifying fields from a "Restricted-Use Data" file *does not* create a "Public-Use Data" file. Disaggregations of "Restricted-Use Data", even without explicit identification fields, may result in a record where the identity of the subject could be reasonably inferred and is prohibited pursuant to this Agreement.

VIII. PROPRIETARY RIGHTS

A. Data Trust Member shall maintain ownership over its own data as well as any methodologies and code developed using only its own data, except for the code, software, or algorithms developed by the Trustee specific to Data Trust Member data necessary to support and maintain the Trust and approved Projects and Uses.

B. Trustee is not required to license or incorporate anything into software that Trustee reasonably believes would infringe a Data Trust Member's intellectual property rights or that Trustee is not authorized to license.

C. Data Trust Users shall maintain ownership over any methodologies developed during the course of their approved Projects and Uses, unless otherwise agreed on by all Parties.

D. All developments, discoveries, inventions, improvements, and modifications (whether or not patentable) conceived and reduced to practice in carrying out Projects and Uses conducted under this Agreement (the "Inventions") will be promptly disclosed by each Party to the other Party. Inventions made solely by employees, agents, consultants, independent contractors or other representatives of the Trustee will be solely owned by the Commonwealth of Virginia. Inventions made solely by employees, agents, consultants, or other representatives of Data Trust User, will be owned solely by Data Trust User, or if the Data Trust User is a state agency, then by the Commonwealth of Virginia. Inventions made jointly by employees, agents, consultants, independent contractors or other representatives of the Trustee and/or employees, agents, consultants, or other representatives of Data Trust User will be owned jointly by the jointly contributing Parties.

E. This Agreement does not transfer from one Party to the other any intellectual property rights that existed prior to this Agreement or that are created independently of this Agreement.

IX. REPRESENTATIONS

A. Each Party represents and certifies that:

i. It has the right and necessary authority to enter into this Agreement.

ii. It has obtained all necessary consents, waivers, and permission to fulfill the purposes contemplated by this Agreement. For the avoidance of doubt, Trustee shall only facilitate the transmission of data only to the extent that the subject data is an Approved Use in the agreement between the Trustee and the Data Trust Member. It is the Data Trust Member's responsibility to obtain all necessary consents and otherwise comply with applicable law in allowing the Trustee to transmit Restricted-Use Data to the Data Trust User and to ensure that the Data Trust Member Agreement provides the necessary information to permit the Trustee to perform its obligations pursuant to this Agreement. The Trustee shall only facilitate the transmission of Restricted-Use Data to the Data Trust User once it has obtained all necessary consents, waivers and permission to transmit the Restricted-Use Data.

iii. Violations of this Agreement shall require the immediate return to Trustee or written verification of destruction of all Restricted-Use Data.

X. LIABILITY

A. The Trustee shall not be liable for any action taken or omitted by it in good faith and believed by it to be authorized hereby or within the rights or powers conferred upon it hereunder, and shall not be liable for any mistake of fact or error of judgment or for any acts or omissions of any kind unless caused by willful misconduct or gross negligence.

XI. INDEMNIFICATION

A. Except if Data Trust User is a Public body of the Commonwealth of Virginia, Data Trust User agrees to indemnify, defend and hold harmless the Commonwealth of Virginia, the Trustee, Data Trust Members, their officers, directors, agents and employees (collectively, "Indemnified Parties") from and against any and all third-party losses, damages, claims, demands, proceedings, suits and actions, including any related liabilities, obligations, losses, damages, assessments, fines, penalties (whether criminal or civil), judgments, settlements, expenses (including attorneys' and accountants' fees and disbursements) and costs (each, a "Claim" and collectively, "Claims"), incurred by, borne by or asserted against any of Indemnified Parties. Selection and approval of counsel and approval of any settlement shall be accomplished in accordance with all applicable laws, rules and regulations. For Commonwealth of Virginia state agencies, the applicable laws include §§ 2.2-510 and 2.2-514 of the Code of Virginia. In all cases involving the Commonwealth or state agencies, the selection and approval of counsel and approval of any settlement shall be satisfactory to the Commonwealth.

XII. CONFIDENTIALITY

A. In performance of this Agreement the Parties may disclose to each other, either in writing or orally, information which the disclosing Party deems to be a trade secret, proprietary and/or confidential (hereinafter, "Confidential Information") and not shared with the Data Trust, but may be necessary for the Trustee and Data Trust User to perform their duties.

B. Confidential Information shall be maintained in confidence during the term of this Agreement and for a period of three (3) years following the termination of this Agreement, except to the extent that it is required to be disclosed by law. After such time, Confidential Information shall be destroyed.

C. Confidential Information does not include information which is (i) known by the Trustee or other Data Trust Users prior to disclosure to them; (ii) generally available to the public other than as a result of breach of this Agreement; (iii) made available to the Trustee or other Data Trust Users by any independent third party who has the right to disclose the information; (iv) information that is published; (v) is independently developed by the Trustee or other Data Trust Users; or (vi) is required to be disclosed by law or a court of competent jurisdiction.

D. In such a case where legal notice of disclosure is received, the Trustee will advise the Data Trust User prior to disclosure so that the Data Trust User will have an opportunity to seek a protective order or other appropriate relief.

E. No Party shall disclose Confidential Information to any third party, and each Party shall keep strictly confidential all Confidential Information of the other. Using reasonable means, each Party shall protect the confidentiality thereof with at least the same level of effort that it employs to protect the confidentiality of its own proprietary and confidential information of like importance. Each Party receiving any such Confidential Information may, however, disclose any portion of the Confidential Information of the other Party to such representatives of the receiving Party as are engaged in a use permitted by this Agreement and have a need to know such portion, provided that representatives: (i) are directed to treat such Confidential Information confidentially and not to use such Confidential Information other than as permitted hereby or subsequently approved by the disclosing Party, and (ii) are subject to a legal duty to maintain the confidentiality thereof. No receiving Party shall use the Confidential Information of a disclosing Party except solely to the extent necessary in and during the performance of this Agreement, as expressly licensed hereunder, or subsequently through approved updates to this Agreement by a disclosing party. The receiving Party shall be responsible for any improper use or disclosure of any of the disclosing Party's Confidential Information by any of the receiving Party's current or former representatives, employees or agents.

XIII. PUBLICATION

A. Subject to the conditions of this Agreement, Data Trust User may publish product(s) produced under this Agreement, provided such publication does not disclose Restricted-Use Data of Data Trust Members. Data Trust User shall not publish any product(s), Confidential Information or any data (including Restricted-Use Data) of the Data Trust without the express written approval of the Trustee. Data Trust User agrees and recognizes that the Trustee is under no obligation to provide approval of the product(s) produced under this Agreement.

B. Prior to submission of all product(s) describing any results for publication, the Data Trust User shall submit the product(s) to the Trustee for review. The Trustee shall then forward the product(s) to all Data Trust Members and Data Trust Members shall have thirty (30) days to determine whether: the product(s) contain(s) Confidential Information; the product(s) contain(s) Restricted-Use Data; and whether a patent application or other intellectual property protection should be sought prior to publication in order to protect the Data Trust Member's proprietary interests in any product or invention developed in connection with the approved Project.

C. In the event that a Data Trust Member notifies the Trustee, or the Trustee determines, that pursuant to Subsection (B) the product(s) contain(s) Confidential Information or Restricted-Use Data, then the Data Trust User shall remove Confidential Information and Restricted-Use Data from the product(s). The Data Trust User shall thereafter resubmit the product(s) for review pursuant to Subsection B.

D. In the event that a patent application or other intellectual property protection is required, then the Trustee, with reasonable justification, shall withhold approval of such publication to obtain patent or other intellectual property protection. Neither Party shall use the name of the other Party, or the name(s) of the other Party's employees, logos, trademarks or other identifiers, without the prior written consent of the other Party, except that the Data Trust User may list the Trust as a resource on any published product(s) after final approval.

E. On request, the Data Trust User shall promptly provide an acknowledgment or assignment in a tangible form satisfactory to the Commonwealth to evidence the Commonwealth's ownership of specifically identified intellectual property created or developed in the performance of this Agreement. The Data Trust User shall provide to Trustee all results, analysis, products, or other information developed using Restricted-Use data made available under this Agreement only in summary or statistical form so that the identity of individuals contained in the Restricted-Use Data is not revealed. The Trustee shall make such reports available to the public in accordance with state public records laws. The Data Trust User shall provide Trustee with all published reports using findings from data provided through this Agreement in a form specified by the Trustee.

XIV. ETHICAL USE

A. Parties agree to abide by a set of ethical principles around data trust creation, management, and use (Exhibit F).

B. Ethical commitments enumerated in this Agreement may be updated through unanimous vote by the Data Governance Council. Any approved changes or additions by the Data Governance Council are applicable to all Data Trust Members, Trustee, and Data Trust Users within thirty (30) days of modification. Trustee must update the ethical commitments enumerated in this Agreement within 7 days of Data Governance Council approval and send electronic notice to all Data Trust Members and Data Trust Users of the changes to the ethical obligations within 14 days of approval.

XV. TERM AND TERMINATION

A. The initial term of this Agreement shall commence on the Effective Date and will remain in effect for two (2) years thereafter unless otherwise modified by mutual agreement. Any Party may terminate their involvement in this Agreement without cause upon thirty (30) days' prior written notice to the other Party. Upon termination Trustee may elect to have the Data Trust User destroy any Restricted-Use Data that it received from the Data Trust.

B. Data Trust User may also renew the Agreement for an additional two (2) year period at any time via written or electronic communication with Trustee.

XVI. MISCELLANEOUS.

A. Amendments. Except as otherwise expressly provided herein, this Agreement may not be modified, amended, or altered in any way except by a written agreement signed by the Parties or electronic consent provided by Parties.

B. Assignment. Neither Party may assign this Agreement or delegate any of its duties, in whole or in part, unless required to by law.

C. Counterparts. This Agreement may be executed in multiple counterparts, each of which shall be deemed an original and all of which together shall be deemed the same agreement.

D. Force Majeure. Neither Party shall be liable for any failure or delay in performing its obligations under this Agreement, or for any loss or damage resulting therefrom, due to acts of God, the public enemy, terrorist activities, riots, fires, and similar causes beyond such Party's control.

E. Governing Law. This Agreement is governed by and will be construed in accordance with the laws of the Commonwealth of Virginia without regard to that body of law

controlling choice of law. Any and all litigation relating to this Agreement must be brought in the circuit courts of the Commonwealth of Virginia.

F. Publicity. Neither Party shall make reference to the other Party in a press release or any other written statement in connection with the Project without the other Party's prior consent, which consent shall not be unreasonably withheld. If there is no notice or disapproval within 5 business days after delivery to the other Party for its review, the material shall be deemed approved. Notwithstanding the foregoing, Trustee shall be permitted to use Data Trust User's name in a list of Data Trust Users that may also include a brief description of the Data Trust's goals and priorities.

G. Severability. Invalidity of any term of this Agreement, in whole or in part, shall not affect the validity of any other term. The Data Trust User and Trustee further agree that in the event such provision is an essential part of this Agreement, they shall immediately begin negotiations for a suitable replacement provision.

H. Survival. Any provisions of this Agreement regarding Proprietary Rights and Confidentiality, Liability, Indemnification and Publication shall survive the expiration or termination of this Agreement.

I. Entire Agreement. The following Exhibits, including all subparts thereof, are attached to this Agreement and are made a part of this Agreement for all purposes:

Exhibit A – Description of the Proposed Project

Exhibit B – Data Protection Security Plan for Restricted-Use Data

Exhibit C – Data Trust Individual User Non-Disclosure Agreements and Non-Disclosure Registry

Exhibit D – Agency Supplied Terms

Exhibit E – List of Requested Data Elements

Exhibit F – Ethical Principles

This Agreement and its Exhibits constitute the entire agreement between the Parties and supersede any and all previous representations, understandings, discussions or agreements between the Parties as to the subject matter hereof. In the event of a conflict, this Agreement shall take precedence over the terms and conditions of any Exhibits. The Parties each acknowledge that it has had the opportunity to review this Agreement and to obtain appropriate legal review if it so chose.

Signatures

Each party to this Agreement certify, by his/her signature, that:

1. The organization identified below has the authority to undertake the commitments in this Agreement; and

2. The signatory has the authority to bind the organization and the named individuals in Exhibit A to the provisions of this Memorandum of Agreement.

Data Trust User Organization [Data Trust User]	**Commonwealth of Virginia Chief Data Officer [Trustee]**
By:	By:
Name:	Name:
Title:	Title:
Date:	Date:

EXHIBIT A: DESCRIPTION OF THE PROPOSED PROJECT

Restricted-Use Data is provided through a Commonwealth of Virginia Data Trust User Sharing Agreement limiting access only to specific organizations and specific personnel for specific purposes under specific security conditions. This Exhibit shall become part of the Agreement and will provide a description of how the Restricted-Use Data will be used.

Data Trust User Organization:

Name of the Principal Project Officer:

Project Title:

Project Statement:

1. State the purpose of the project including goals and objectives.
2. Describe the intended use of the findings including expected publications and/or derived products.
3. Why are Restricted-Use data required to meet the desired goals of the project?
4. Describe how the stated goals and objectives align with Commonwealth of Virginia Goals.
5. Identify stakeholders that will access project products.
6. Explain the importance of the project and describe any anticipated results

Authorized Personnel

The Data Trust User will ensure access to the Restricted-Use Data will be limited to the personnel specified in this Agreement and that individual records are accessed solely for the purpose authorized. The Data Trust User must also ensure that all personnel authorized to access Data Trust data will have undergone a satisfactory criminal background check within two (2) years prior to granting access. The Data Trust User is responsible for maintaining a list of authorized personnel who have access to the data and keeping the Trustee informed of any changes to the list.

Employee, Contractor, or Agent Name	***Position or Title***

EXHIBIT B: DATA PROTECTION SECURITY PLAN FOR RESTRICTED-USE DATA

Provide a brief description of the computer system, software, and network that will be used to store, manipulate, and analyze the Restricted-Use Data by answering the questions provided below. Logical and technical system diagrams are required for all networked installations. Organizations are encouraged to attach additional documentation of their information security policies and procedures.

Restricted-Use Data cannot be stored in any cloud file storage service (e.g., Google Drive, Dropbox, etc.) unless the cloud service has been assessed and approved for operation by VITA's Enterprise Cloud Oversight Service (ECOS). It is preferred and recommended that restricted data be stored and accessed from a secure server completely controlled, managed, secured, and audited by the Data Trust User.

If Commonwealth agency: [AGENCY NAME] follows and complies with all Commonwealth of Virginia information security policies, practices, and standards as defined by SEC-501, SEC-525 and monitored by the Virginia Information Technologies Agency (VITA).

If using the Secure Data Enclave: [ORGANIZATION NAME] will access the Restricted-Use data only through the Secure Data Enclave which follows and complies with all Commonwealth of Virginia information security policies, practices, and standards as defined by SEC-525 and monitored by the Virginia Information Technologies Agency (VITA).

Question	***Response***
Where will the restricted data be stored and how will the data files be encrypted?	
How often do you update and review access policies for all system users and administrators?	
Please provide the date of your most recent access policy review.	
Describe the procedures for limiting access to systems and data files to only authorized team members.	
Can data import, data export, and service management be conducted over secure industry accepted standardized network protocols? How will data be securely transmitted between team members (if applicable) within and external to your network?	
Describe the procedures in place to ensure restricted use data shall not be replicated or used in non-secure environments.	
Do you conduct network, application, and operating system layer vulnerability scans? Please provide the scanning frequency.	

Do you utilize industry standard malware protection on all systems with access to restricted data?	
What software will be used to visualize, analyze, and report results generated from the data?	
Where will the files generated by the visualization, analysis, and intelligence software be stored and how will the files be protected?	
Do you specifically train your employees, contractors, or agents regarding their specific roles and the information security controls they must fulfill?	
Please describe your training requirements and how you document employee acknowledgement of training.	
Do you audit your security practices or conduct security assessments annually? Are the results of internal and external audits available for review?	
Please provide the date of your most recent audit or security assessment.	
Do you conduct risk assessments associated with data governance requirements at least once a year?	
Please provide the date of your most recent risk assessment.	
Are the results of your most recent risk assessment available for review?	
Do you have controls in place to restrict and monitor the unauthorized movement of data within your systems?	
Please describe your backup strategy and data retention policies.	
Do you support secure deletion of archived and backed-up data?	
Do you have a documented security incident response plan?	
Please provide the date of your most recent test of your security incident response plan.	
Do you have a defined and documented incident notification process for reporting suspected security	

incidents within 24 hours?	

EXHIBIT C: DATA TRUST INDIVIDUAL USER NON-DISCLOSURE AGREEMENT

This **Commonwealth of Virginia Data Trust Individual User Non-Disclosure Agreement (Non-Disclosure Agreement)** is made effective as of the ____ day of _____, 20__, by and between the Chief Data Officer for the Commonwealth of Virginia as the Trustee of the Commonwealth of Virginia's Data Trust ("Trustee") and _____, an employee, contractor, or agent of the Data Trust User ("Data Trust Individual User").

The Trustee has entered into the Commonwealth of Virginia Data Trust User Agreement (Data Trust User Agreement) with the Data Trust User. The Data Trust User will utilize data from the Commonwealth of Virginia Data Trust. The Data Trust User has identified the project and usage of the data in the Exhibits to the Data Trust User Agreement. The Data Trust User has identified the Data Trust Individual User as a member of the project.

The Data Trust User and the Data Trust Individual User hereby agree to adhere to all terms of the Data Trust User Agreement and the Exhibits, including this Exhibit C. The Data Trust Individual User hereby certifies that he or she has been provided the Data Trust User Agreement with the Exhibits and will comply with all of the Data Trust User Agreement's provisions.

The Data Trust Individual User agrees that the data, information and documentation provided by the Data Trust is to be considered Confidential Information and is proprietary to the Commonwealth. The Data Trust Individual User shall hold Confidential Information and any data from the Data Trust in confidence. The Data Trust Individual User shall not disclose, publish or otherwise reveal any of the Confidential Information received from the Commonwealth or the Project outside of the project's other employees, agents, or subcontractors whatsoever except pursuant to the terms of the Data Trust User Agreement.

The Data Trust Individual User shall not, without specific prior written authorization of the Data Trust User, relocate or remove any Confidential Information from the project office.

Data Trust Individual User agrees that Confidential Information accessed by or in his/her possession shall be protected and stored pursuant to the Data Protection Security Plan in Exhibit B.

Any Data Trust Individual User who is assigned to the Project and is a party to this Non-Disclosure Agreement will be immediately dismissed from the Project in the event of any breach or threatened breach of this Non-Disclosure Agreement by such Data Trust Individual User or in the event that the Data Trust Individual User causes the Data Trust User to breach its Data Trust User Agreement with the Trustee.

IN WITNESS WHEREOF, the parties have executed this Non-Disclosure Agreement effective as of the latter date below:

[Data Trust Individual User]	**[Trustee]**
By:	By:
Name:	Name:
Title:	Title:
Date:	Date:

EXHIBIT D: AGENCY SUPPLIED TERMS

Restricted-Use data is provided through a Data Trust User Sharing Agreement limiting access only to specific organizations and specific personnel for specific purposes under specific security conditions.

This Exhibit shall become part of the Agreement and provides the additional terms below:

EXHIBIT E: LIST OF REQUESTED DATA ELEMENTS

The following is a list of data elements included in this Agreement as approved by each Data Trust Member:

DATA TRUST MEMBER:

DATA ASSET NAME:

DATA ELEMENT	DESCRIPTION
DATA ELEMENT 1	DESCRIPTION 1

EXHIBIT F: ETHICAL PRINCIPLES

All individuals participating in the data trust or utilizing data trust resources, including Data Governance Council Representatives, Data Trust Members, Data Trust Users, Executive Data Board Members, Trustee, or any other individual utilizing data trust resources shall adhere to the following ethical principles when handling Data provided to the Trust as detailed in Exhibit B for the allowable uses and projects outlined in Exhibit A:

A. Respect

1. Parties shall consider whether the insights gleaned from use of the data could unfairly limit an individual's or a community's opportunities
2. Parties shall not use data in a way that could stigmatize or portray demographic groups, cultures, or communities in terms of deficit.
3. Parties assessing the ethical benefits and harms of data use should conduct assessments from the perspective of the individuals, groups, or communities to whom the data relate.
4. Parties shall actively work to mitigate the potential harm to individuals and communities that could occur from use of the data.
5. Parties shall actively work to understand, mitigate, and communicate the presence of bias in the data.

B. Privacy

1. Parties shall make every effort to guarantee the security of data, subjects, and algorithms to prevent unauthorized access, disclosure of sensitive information, policy violations, tampering, or harm to data subjects.
2. Parties shall make every effort to protect anonymous data subjects, and any associated data, against any attempts to reverse-engineer, de-anonymize, or otherwise expose confidential information.

C. Transparency

1. Parties shall work to implement and maintain auditability in all uses of data.
2. Parties shall make every effort to provide mechanisms for tracking the context of collection, methods of consent, the chain of responsibility, and assessments of quality and accuracy of the data, where applicable.
3. Parties shall establish consistent review practices for data and process auditability.
4. Parties shall provide sufficient context and documentation to enable other trained parties or practitioners to evaluate the use of data.
5. Parties shall ensure that metadata acknowledges the provenance and purpose and any limitations or obligations in secondary use inclusive of issues of consent.

D. Openness

1. Parties shall work to include representation from relevant data subjects or communities, where applicable
2. Parties shall work to foster diversity by ensuring inclusion of a variety of communities and philosophies when working with data.
3. Parties shall engage in responsible communication with stakeholders of data resources, considering and providing clear opportunities for feedback from all stakeholders.

E. Integrity

1. Parties shall use data in ways that are consistent with the intentions and understanding of the disclosing party.
2. Parties shall make every effort to ensure that future use of the data conforms with the intentions and understanding of the disclosing party.
3. Parties shall acknowledge and disclose caveats and limitations to the process and outputs.